

REMARKS

Claims 1-20 are pending in this application, all of which have been rejected. Claim 16 has been objected to as claiming dependency from itself. Claims 5-7 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 1-20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Garrison (US 6,336,114) in view of Yamamoto et al. (US 2001/0044903). Entry of the claim amendments and reconsideration of claims 1-20 is respectfully requested.

Amendments to the Claims

Claims 1-11, 14-16, 18, and 20 are amended herein. For consistency, instances of “said” have been replaced by “the” throughout the claim set. Claim 2 has been amended to add “a” before “data storage device” for better grammatical sense. Similarly, claim 4 has been amended to add the inadvertently omitted word “by” to the phrase “when the access requests are processed by the local servers” also for better grammatical sense. These amendments to claims 2 and 4, and the replacements of “said” with “the” throughout the claim set, are not made to overcome rejections of the amended claims and should not create an estoppel with respect to any later determination of equivalents under the Doctrine of Equivalents. Claims 5 and 6 have been amended to replace “can be” with “comprises,” and claim 7 has been amended to replace “can be” with “are.” Claim 16 has been amended to depend from claim 10 rather than itself, and the dependencies of other claims have also been amended where such amendments serve to broaden claim scope.

Claim Objections

In paragraph 2, claim 16 has been objected to as claiming dependency from itself. As claim 16 is amended herein to depend from claim 10, Applicants request that the Examiner withdraw the objection to claim 16.

Claim Rejections under 35 U.S.C. §112, Second Paragraph

In paragraphs 3 and 4, claims 5-7 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Specifically, “can” and “can be” have been deemed to render the

claims indefinite because it is unclear whether the limitations following these words are part of the claimed invention. The amendments to claims 5-7 noted above make these claims definite within the meaning of 35 U.S.C. §112, second paragraph. Applicants therefore request that the Examiner withdraw the 35 U.S.C. §112, second paragraph, rejections of claims 5-7.

Claim Rejections under 35 U.S.C. §103(a)

Claims 1-20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Garrison in view of Yamamoto et al. Independent claim 1 recites a distributed access control system. The system comprises a central server and a plurality of local servers. The central server has “a server module that provides overall access control,” and the local servers each include “a local module that provides local access control.”

Per MPEP §2111, “[d]uring patent examination, the pending claims must be ‘given their broadest reasonable interpretation consistent with the specification.’ *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000).” Likewise, MPEP §2106(C) states that “[o]ffice personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. *In re Morris*, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997).” According to the present specification, “[e]ach of local servers 104...manage those users who are local to respective local servers 104” (paragraph [0044]). The embodiment shown in FIG. 1B of the specification shows that each local server 104 is coupled, by a LAN 110, to one or more clients 102 that are local to the particular server 104. In light of the supporting disclosure, it is clear that the broadest reasonable interpretation of a local server is a server that is dedicated to a distinct population of local clients.

The Examiner has apparently equated the servers 17a and 17b of Garrison with the claimed local servers, based on the subject matter of the paragraphs of Garrison cited by the Examiner. The servers 17a and 17b of Garrison are not local servers, under the broadest reasonable interpretation, because the servers 17a and 17b are not each dedicated to distinct populations of local clients. Rather, both servers 17a and 17b serve the same client 14. Moreover, Garrison notes that “[t]he client 14 is preferably a computer system located remotely from the server 17a.” “[R]emotely located” “refer[s] to a location separated from the premises of the server 17a by an unsecure connection” (col. 3 lines 11-16). Thus, client 14 is not local to server 17a. Additionally, claim 1 requires a plurality of local servers, and Garrison teaches only

a single server 17a; server 17b is deemed to be a remote server by Garrison (see FIG. 2) because server 17b is associated with a remote database (col. 7 lines 65-67).

Turning to Yamamoto et al., the Examiner asserts that Yamamoto et al. “teaches a distributed access control system” (paragraph 8 page 3). Applicants disagree. Yamamoto et al. does not discuss “access control.” For the most part, the term “access” is used by Yamamoto et al. as a noun, e.g. “the contents of *the* access” (paragraph [0025], emphasis added), and “[a]ccess referred to herein embraces various instructions such as indications made by FAX and printing commands, as well as request for information and gaining of information” (paragraph [0021]).

Yamamoto et al. does note that “it is an object of the present invention to provide an information access method” (paragraph [0018]), but the method has little to do with controlling access to the information and is not distributed. To the extent that access to information is controlled, it is controlled by a firewall (“Because the segments Sa-Se where the host servers 10a-10e are respectively positioned are protected by the firewall 11, it is difficult for an unauthorized person to access the housing.” (paragraph [0086])). Authentication at log-in is determined by proper user ID and password (paragraph [0139]).

Yamamoto et al. does not discuss restrictions or limitations on access to specific files or records, and notes only that “the system administrator registers various conditions (i.e., protocols, data format intrinsic in the system, the address of the host server 10, etc.) under which the firewall 11 allows access from the originator terminal” (paragraph [0106]). To the extent that “various conditions” may pertain to restrictions on access to particular information, such access is controlled by the firewall 11. Thus, access control in Yamamoto et al. is centralized in the firewall 11, and not distributed.

Furthermore, the Examiner apparently has equated the host servers 10 of Yamamoto et al. with the central server of claim 1, based on the subject matter of the paragraphs of Yamamoto et al. cited by the Examiner. Yamamoto et al., however, does not disclose that the host servers 10 include modules, let alone a server module that provides overall access control. Rather, as noted above, access control is vested in the firewall 11 and not the host servers 10.

Since Garrison and Yamamoto et al. do not teach between them every limitation of claim 1, the two references cannot provide the basis for a *prima facie* case of obviousness. Even if, *arguendo*, the two references do teach each of the limitations, there is no motivation to combine the references. Whereas Garrison deals with restricting access to particular rows of a requested

column of a database table (col. 2 lines 21-25), Yamamoto et al. deals with making files located on local servers available for access from cellular phones by placing an intranet, including a firewall, between the cellular network and the local servers (see Abstract and FIG. 1). Clearly, the two references bear only a superficial relationship to one another.

One of ordinary skill in the art at the time of the invention would have recognized that the system of Garrison is specifically intended to provide security over an unsecured connection (“FIG. 1 depicts a client/server system 10 *illustrating the principles of the present invention*. Referring to FIG. 1, a client 14 is configured to communicate with a server 17a via communications network 18. *The client 14 is preferably a computer system located remotely from the server 17a, which is preferably a computer system as well. As used herein, the terms "remotely located" or "remote location" shall refer to a location separated from the premises of a server 17a by an unsecure connection. An unsecure connection is any connection accessible by a hacker or unauthorized user.*” (col. 3 lines 9-19)).

The Examiner suggests a proposed modification to Garrison that would “improve the functionality of Garrison’s system by allocating a central server to authorize and grant access to the overall network therefore increasing security and protecting digital assets” (paragraph 9 page 4). However, one of ordinary skill in the art at the time of the invention would have viewed such a modification as unnecessary as the system of Garrison already secures digital assets from unauthorized users and hackers. Applicants note that, per MPEP §2143.01, “[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination” citing *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430, 562 (Fed. Cir. 1990). Here, the proposed modification of Garrison adds extra components, complexity, and cost to the system of Garrison without a benefit, and therefore one of ordinary skill would have viewed the combination as distinctly lacking desirability.

Applicants also note that the Examiner failed to particularly describe the proposed modification of the system of Garrison according to the teaching of Yamamoto et al. The Examiner states that “[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Yamamoto and Garrison because they both deal with providing and restricting access to data over a communications network” and “a central server having a server module that provides overall access control and a plurality of local servers

would improve the functionality of Garrison's system by allocating a central server to authorize and grant access to the overall network" (paragraph 9 pages 3-4), but this does not particularly describe which components of Yamamoto et al. the Examiner proposes to add to the system of Garrison, or where those components are supposed to be located.

As Garrison does not teach a plurality of local servers, and Yamamoto et al. does not teach a distributed access control system comprising a central server having a server module that provides overall access control, and even if, *arguendo*, the references did teach these limitations one of ordinary skill would not have found it desirable to combine the references, Applicants request that the Examiner withdraw the 35 U.S.C. §103(a) rejections of claim 1, and claims 2-9 depending therefrom.

Independent claim 10 has been rejected under 35 U.S.C. §103(a) over Garrison in view of Yamamoto et al. Applicants note, however, that the specific rejection of claim 10, and of several dependent claims, makes no mention of Yamamoto et al. The form of these rejections appears to be in error. Accordingly, Applicants will discuss such claims as if rejected as anticipated by Garrison.

With respect to claim 10, the claim recites a method comprising "reconfiguring a first server machine to prevent further access by a user to secured items via the first server machine," and "reconfiguring a second server machine to permit access by the user to at least the secured item via the second server machine." Garrison does not teach any such reconfigurations. The Examiner cites to col. 12 lines 16-46 of Garrison for the teaching of reconfiguring the first server machine. Applicants note, however, that the cited paragraphs of Garrison teach alternative strategies that can be employed by server 17a ("the server 17a *first* consults the security data table 57" (col. 12 lines 18-19) and "the server 17a can consult the security data table 57 *after* retrieving the data" (col. 12 lines 34-35) emphasis added in both). Garrison, however, does not teach reconfiguring the server 17a to switch between these alternatives. The implication of Garrison is that these alternatives work equally well, as Garrison does not provide a preference or describe circumstances where one is more desirable than the other. Thus, once the server 17a is configured with a set of rules there is no reason to reconfigure the server 17a.

Likewise, reconfiguring the second server machine required by claim 10 also is not taught by Garrison. The Examiner cites to col. 8 lines 10-51 of Garrison for teaching

reconfiguring the second server machine. However, the cited paragraph merely details the process that transpires when the server 17a has to retrieve data from the remote server 17b. Nowhere does Garrison teach or suggest that the remote server 17b is reconfigured in this process.

It is also worth noting that taken together, the two reconfiguration steps of claim 10 amount to a transfer of secured data access from the first server machine to the second. Accordingly, though further access by the user to secured items via the first server machine is prevented in one step, in the other step, access by the user to at least the secured item via the second server machine is permitted. Clearly, at least the same secured item exists on both the first and second server machines, and access to the secured item is being transferred.

In contrast, the system of Garrison only employs the remote server 17b to access data that is not available locally to the server 17a in database system 19a (“Once the server 17a receives the data from the database system 19a, the server 17a determines whether a remote server 17b has access to any of the requested data not included in the database system 19a” (col. 12 lines 47-50)). In Garrison, access to the same secure data isn’t transferred from one server to another, rather, access to different secure data may be simultaneously available through both a local and a remote server.

For at least these reasons, Garrison does not anticipate claim 10 and Applicants request that the Examiner withdraw the 35 U.S.C. §103(a) rejections of claim 10, and claims 11-17 depending therefrom.

Applicants note the further patentability of claim 11. Claim 11 adds the limitation to claim 10 that “authenticating (a) authenticates both the user and a client machine being used by the user.” However, Garrison does not teach additionally authenticating the client 14. Garrison provides that “the server 17a can be configured to determine whether the user is authorized to access the requested data” and “is configured to discard any data determined by the server 17a to be inaccessible to the user of the client 14” (col. 7 lines 31-42), but here the authorization, or lack thereof, rests solely in the user and not in the client. Thus, the client 14 is not authenticated.

Applicants note the further patentability of claims 13 and 15-17. In the rejections of each of these claims the Examiner relied on Yamamoto et al. for teachings not found in Garrison. For at least the reasons provided above with respect to claim 1, one of ordinary skill in the art at the

time the invention was made would not have been motivated to combine Garrison and Yamamoto et al.

Independent claim 18 has been rejected under 35 U.S.C. §103(a) over Garrison in view of Yamamoto et al. Applicants note here, too, that the specific rejection of claim 18 makes no mention of Yamamoto et al. Claim 18 recites a computer readable medium including "at least computer program code for providing access management through use of a plurality of server machines associated with different locations, the computer readable medium comprising computer program code" for each of the limitations of claim 10. For at least the reasons provided above with respect to claim 10, applicants request that the Examiner withdraw the 35 U.S.C. §103(a) rejections of claim 18 and claims 19 and 20 depending therefrom.

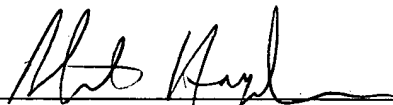
All pending claims are allowable and Applicants therefore respectfully request a Notice of Allowance from the Examiner. Should the Examiner have questions, the Applicant's undersigned agent may be reached at the number provided.

Respectfully submitted,

Hal Hildebrand et al.

Date: 7/29/2005

By:


Robert Hayden, Reg. No. 42,645
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
TEL: (650) 812-3465
FAX: (650) 812-3444